BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : H04L 29/06, 12/24, G06F 9/44 — A1

(11) Numéro de publication internationale: **WO 99/21335**

(43) Date de publication internationale: 29 avril 1999 (29.04.99)

(21) Numéro de la demande internationale: PCT/FR98/02218

(22) Date de dépôt international: 15 octobre 1998 (15.10.98)

(30) Données relatives à la priorité:
97/13254 16 octobre 1997 (16.10.97) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: SOLSOFT [FR/FR]; 4, bis rue de la Gare, F-92300 Levallois-Perret (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: FOUGERAT, Jérôme [FR/FR]; 7, rue Valentin Haüy, F-75015 Paris (FR).

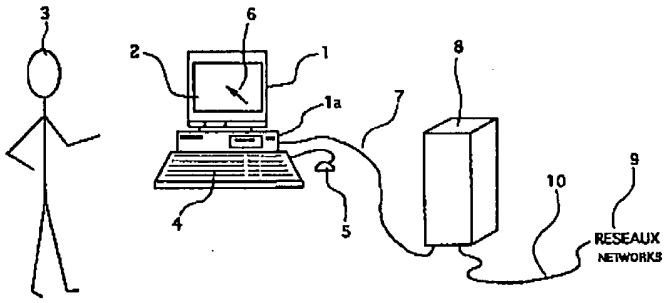
(74) Mandataire: VIDON, Patrice; Cabinet Patrice Vidon, Immeuble Germanium, 80, avenue des Buttes de Coësmes, F-35700 Rennes (FR).

(81) Etats désignés: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée
Avec rapport de recherche internationale.

(54) Title: METHOD FOR GENERATING FILTERS DESIGNED TO AVOID RISKS OF BREACH IN INTERCONNECTED COMPUTER NETWORKS

(54) Titre: PROCEDE POUR GENERER LES FILTRES DESTINES A EVITER LES RISQUES D'INTRUSION DES RESEAUX INFORMATIQUES INTERCONNECTES



(57) Abstract

The invention concerns the field of interconnected computer networks, consisting in a system for generating in a simple and automatic way filters, according to the internet protocol, designed to avoid the risk of breach in interconnected computer networks. A computer terminal (1) and control means (4, 5) interact iteratively with a graphic interface (2) so as to: generate and display the objects and classes requiring security; select and display the application protocols for which filters need to be generated; draw on the graphic interface, by means of arrow curves for each application protocol previously selected, the communication laws. The terminal (1) comprises computing means (1a) for converting the graphic data representing the communication laws into programming data for the screening routers (8).

(57) Abrégé

Le domaine de l'invention est celui des réseaux informatiques interconnectés. Le système selon l'invention a pour objet de générer de manière simple et automatique les filtres, selon le protocole internet, destinés à éviter les risques d'intrusion des réseaux informatiques interconnectés. Un terminal de calcul (1) et des moyens de commande (4, 5) interagissent de manière itérative avec une interface graphique (2) pour: créer et visualiser les objets et les classes du domaine de sécurité, sélectionner et visualiser les protocoles d'application pour lesquels des filtres doivent être créés, dessiner sur l'interface graphique, au moyen de courbes fléchées pour chaque protocole d'application préalablement sélectionné, les lois de communication. Le terminal (1) comprend des moyens de calcul (1a) pour convertir les données graphiques représentatives des lois de communication en données de programmation des routeurs filtrants (8).

Procédé pour générer les filtres destinés à éviter les risques d'intrusion des réseaux informatiques interconnectés.

Le domaine de l'invention est celui des réseaux informatiques interconnectés.

Le caractère ouvert des réseaux informatiques selon le protocole Internet offre bien des facilités. Toutefois, il apporte aussi son lot de dangers, risques d'intrusion des réseaux, difficultés pour se protéger. Il existe des matériels et des logiciels permettant d'effectuer un filtrage des paquets utilisant le protocole Internet. Toutefois, la maîtrise de ce filtrage pour l'application de politiques de sécurité exigeantes est difficile et complexe.

L'invention concerne un procédé pour générer de manière simple et automatique les filtres, utilisant le protocole Internet, destinés à éviter les risques d'intrusion des réseaux informatiques interconnectés.

Les termes qui seront ci-après utilisés pour exposer la solution technique selon l'invention, ont les définitions suivantes :

- On désigne par "réseau" un ou des intervalles fermés (au sens topologique du terme) d'adresses du Protocole Internet.
- On désigne par "objets" les éléments constitutifs d'un réseau. Ainsi, sans que cette énumération soit exhaustive, sont des objets au sens de la présente invention : les ordinateurs, les équipements informatiques, les serveurs, les imprimantes, les réseaux (physiques ou logiques), les sous-réseaux (physiques ou logiques), les équipements de filtrage, les pare-feu, les utilisateurs ou groupes d'utilisateurs, les applications informatiques. Un objet est caractérisé par son type et par son nom. Par exemple un routeur filtrant est un type d'objet, de même un ensemble de réseaux est un type d'objet. Un objet possède une ou plusieurs adresses ou un ou plusieurs intervalles fermés d'adresses.
- On désigne par "protocole" une convention précisant les règles et les spécifications techniques à respecter dans le domaine des

télécommunications afin d'assurer l'interopérabilité des objets.

- On désigne par "protocole de communication" un protocole, tel que par exemple le protocole Internet, définissant une technique de transfert de données.
- On désigne par "protocole d'application" ou "service" un protocole définissant une technique d'échange de données ou de commandes pour une application définie.
- On désigne par "classe" l'ensemble des adresses ayant les mêmes lois de communication. Une classe peut réunir d'autres classes. Les classes sont des objets au sens de la présente description de l'invention.
- On désigne par "loi de communication" une loi autorisant ou interdisant pour le protocole d'application concerné, la communication entre un couple d'objets, un couple de classes ou un couple mixte (classe, objet).
- On désigne par "domaine de sécurité" un ensemble d'objets interconnectés sur lequel s'applique des lois de communication spécifiques à chaque objet ou générales.
- On désigne par "lien" ou "connexion", les connexions physiques (les câbles des réseaux par exemple) reliant les objets entre eux. Un réseau est un ensemble d'objets interconnectés.
- On désigne par "routeur" un équipement permettant l'interconnexion de réseaux disjoints .
- On désigne par "filtre" les moyens techniques permettant de mettre en oeuvre les lois de communication. Par exemple la programmation d'un routeur permet de contrôler la possibilité de communiquer entre deux réseaux disjoints. Par extension on appelle routeur filtrant tout équipement permettant le filtrage du protocole Internet.

Les objectifs visés par la présente invention, à savoir : la génération de manière

simple et automatique des filtres destinés à éviter les risques d'intrusion des réseaux informatiques interconnectés, sont atteints à l'aide d'un procédé consistant à utiliser de manière itérative une interface graphique pour :

- créer et visualiser les objets et les classes du domaine de sécurité,
- sélectionner et visualiser les protocoles d'application pour lesquels des filtres doivent être créés,
- dessiner sur l'interface graphique, au moyen de courbes fléchées, pour chaque protocole d'application préalablement sélectionné, les lois de communication.

Le dessin de ces courbes fléchées représentatives des lois de communication permet de créer simultanément et instantanément la création des filtres associés aux routeurs filtrants et s'appliquant aux objets concernés. A cet effet et selon une étape complémentaire du procédé :

- on convertit les données graphiques représentatives des lois de communication en données de programmation des routeurs filtrants.

Le procédé selon l'invention permet d'utiliser l'interface graphique pour visualiser la politique de sécurité du domaine de sécurité et pour la modifier le cas échéant. De préférence, on modifie les lois de communication entre objets ou classes sur l'interface graphique en sélectionnant des protocoles d'application prédéterminés.

La présente invention concerne également un système pour générer de manière simple et automatique les filtres, selon le protocole Internet, destinés à éviter les risques d'intrusion des réseaux informatiques interconnectés. Le dit système consiste à utiliser une interface graphique associée à un terminal de calcul et des moyens de commande interagissant avec l'interface graphique pour :

- créer et visualiser les objets et les classes du domaine de sécurité,
- sélectionner et visualiser les protocoles d'application pour lesquels des filtres doivent être créés,
- dessiner sur l'interface graphique, au moyen de courbes fléchées, pour

chaque protocole d'application préalablement sélectionné, les lois de communication.

Le dessin de ces courbes fléchées représentatives des lois de communication permet de créer simultanément et instantanément la création des filtres associés aux routeurs filtrants et s'appliquant aux objets concernés. A cet effet et selon une caractéristique complémentaire, le système comprend des moyens de calcul pour :

- convertir les données graphiques représentatives des lois de communication en données de programmation des routeurs filtrants.

Le système selon l'invention permet d'utiliser l'interface graphique pour visualiser la politique de sécurité du domaine de sécurité et pour la modifier le cas échéant. De préférence, pour modifier les lois de communication entre objets ou classes sur l'interface graphique, les moyens de commande comportent des moyens pour sélectionner des protocoles d'application prédéterminés.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description de variantes de réalisation de l'invention, données à titre d'exemple indicatif et non limitatif, et de :

- la figure 1 présentant une vue schématique en perspective du système selon l'invention ;
- la figure 2 présentant l'écran de visualisation pendant la phase de création des objets et plus particulièrement des réseaux du domaine de sécurité ;
- la figure 3 présentant l'écran de visualisation pendant la phase de création des objets et plus particulièrement des routeurs du domaine de sécurité ;
- la figure 4 présentant l'écran de visualisation après que les liens entre les objets aient été spécifiés (dans le cas représenté le routeur est interconnecté par des liens physiques à cinq réseaux) ;
- les figures 5 et 6 présentant l'écran de visualisation pendant la phase de

création des classes du domaine de sécurité ;

- la figure 7 présentant l'écran de visualisation pendant la phase de sélection des protocoles d'application et de dessin des lois de communication.

On va maintenant décrire la figure 1 qui représente une vue schématique en perspective du système selon l'invention.

Le terminal de calcul 1 comporte un écran de visualisation 2 autrement appelé interface graphique. Le terminal est commandé par l'utilisateur 3 au moyen d'un clavier 4 et d'un boîtier de commande 5 (une souris). Ces organes de commande permettent, de manière usuelle, de déplacer un pointeur 6 sur l'écran de visualisation 2. Le terminal de calcul est interconnecté par une liaison câble 7 à au moins un routeur filtrant programmable 8. Ce routeur est lui même interconnecté aux réseaux 9 par des liens 10 .

On va maintenant décrire la figure 2 qui représente l'écran de visualisation pendant la phase de création des objets et plus particulièrement des réseaux du domaine de sécurité.

La partie droite de la barre d'outil 11 de l'écran de visualisation 2 comporte cinq icônes : 12 sélection, 13 routeur filtrant, 14 réseau, 15 classe, 16 loi de communication, dont on décrira ci-après les fonctions. A gauche de la barre d'outil 11 se trouve les icônes 50 : fichier, édition, couper, coller. De manière usuelle, ces outils permettent, lorsqu'ils sont sélectionnés et activés par le pointeur 6 actionné par le boîtier de commande 5, d'ouvrir des fichiers, d'enregistrer l'interface graphique, d'en couper ou d'en coller des parties.

Une fenêtre ouverte 17 comporte la liste des services 18 autrement appelés protocoles d'application dans la description.

Afin de créer la représentation graphique d'un réseau sur l'interface graphique 2, l'utilisateur utilise la souris 5 pour activer au moyen du pointeur 6 l'icône 14. Les représentations graphiques des réseaux apparaissent sur l'écran de visualisation 2,

sous forme de nuages, 19, 20, etc. Au moyen de l'outil de sélection 12, l'utilisateur peut sélectionner, déplacer et disposer à sa convenance les réseaux. Dans l'exemple représenté, le réseau 20 dénommé "sécurisé" a été sélectionné. En agissant sur le boîtier de commande 5 l'utilisateur peut ouvrir des fenêtres de dialogue 21, 22 sur l'écran 2 afin d'entrer les propriétés du réseau, notamment les adresses 24. L'utilisateur procède de manière itérative pour créer les autres réseaux.

On va maintenant décrire la figure 3 qui représente l'écran de visualisation pendant la phase de création des objets et plus particulièrement des routeurs du domaine de sécurité.

Afin de créer la représentation graphique d'un routeur 25 sur l'interface graphique 2, l'utilisateur utilise la souris 5 pour activer au moyen du pointeur 6 l'icône 13. La représentation graphique du routeur 25 apparaît sur l'écran de visualisation 2. Au moyen de l'outil de sélection 12, l'utilisateur peut sélectionner, déplacer et disposer à sa convenance le routeur 25 sur l'interface graphique 2. Dans l'exemple représenté, le routeur 25 dénommé "routeur" a été sélectionné. En agissant sur le boîtier de commande 5 l'utilisateur peut ouvrir des fenêtres de dialogue 26 sur l'écran 2 afin d'entrer les propriétés du routeur notamment ses spécifications (la marque du constructeur et du logiciel associé) ainsi que les spécifications (les noms) des réseaux avec lesquels le routeur est interfacé. Les liens ou les connexions entre les réseaux 19 "Internet", 20 "Sécurisé", 20a "Dmz", 20b "Central", 20c "Commerce", et le routeur 25 sont représentés sur l'interface graphique 2 par des traits 27, 28, 28a, 28b, 28c (figure 4). L'utilisateur procède de manière itérative pour créer les autres routeurs et spécifier leurs liens avec les réseaux.

On va maintenant décrire les figures 5 et 6 qui représentent l'écran de visualisation pendant la phase de création des classes du domaine de sécurité.

Afin de créer la représentation graphique d'une classe 30 sur l'interface graphique 2, l'utilisateur utilise la souris 5 pour activer au moyen du pointeur 6 l'icône 13. La représentation graphique de la classe 25 apparaît sur l'écran de visualisation 2.

Au moyen de l'outil de sélection 12, l'utilisateur peut sélectionner, déplacer et disposer à sa convenance la classe 30 sur l'interface graphique 2. Dans l'exemple représenté la classe 30 dénommée "classe" a été sélectionnée. En agissant sur le boîtier de commande 5 l'utilisateur peut ouvrir des fenêtres de dialogue 31, 32 sur l'écran 2 afin d'entrer les propriétés de la classe notamment les adresses du réseau "Dmz" 20 appartenant à la classe 30 "classe". Un trait de couleur gris pale 31 permet de visualiser l'appartenance de la classe 20a au réseau "Dmz" 20a (figure 6). La classe 32 dénommée "classe-central-commerce" a été spécifiée de telle sorte qu'elle inclut des adresses du réseau 20b "Central" et des adresses du réseau 20c "Commerce". Aucun trait ne relie la classe 32 "classe-central-commerce" aux réseaux 20b "Central" et 20c "Commerce". On visualise ainsi sur l'interface graphique 2 que la classe 32 "classe-central-commerce" regroupe des objets présents dans les réseaux "Central" et "Commerce". L'écran 2 de la figure 6 représente, dans le cas particulier décrit, le domaine de sécurité ainsi que les objets (réseaux, routeur) et les classes de ce domaine de sécurité. L'utilisateur procède de manière itérative pour créer les autres classes et compléter le domaine de sécurité.

On va maintenant décrire la figure 7 qui présente l'écran de visualisation pendant la phase de sélection des protocoles d'application et de dessin des lois de communication.

L'utilisateur actionne le boîtier de commande 5 pour déplacer le pointeur 6 et sélectionner puis activer dans la fenêtre services (protocoles d'application) 18, le protocole d'application concerné. La liste des protocoles d'application apparaissant dans la fenêtre services 18 est proposée par défaut, l'utilisateur a la possibilité d'en ajouter d'autres. Dans le cas décrit le protocole d'application sélectionné est le protocole 40 "smtp". Par défaut, la" loi de communication ", c'est-à-dire la loi autorisant ou interdisant pour le protocole d'application concerné, la communication entre un couple d'objets, un couple de classes ou un couple mixte (classe, objet) est une loi d'interdiction. Pour définir la politique de sécurité associée au protocole

d'application 40 "smtp" sélectionné, l'utilisateur procède comme il sera ci-après décrit en se référant à deux cas particuliers.

Dans le premier cas, pour mettre en place une loi d'autorisation du réseau "Internet" 19 vers la classe "classe" 30, l'utilisateur utilise la souris 5 pour activer au moyen du pointeur 6 l'icône 16. Il spécifie alors au moyen d'une fenêtre de dialogue qu'il s'agit d'une loi d'autorisation. Ensuite l'utilisateur positionne le pointeur 6 sur le réseau "Internet" 19, actionne le boîtier de commande 5 pour sélectionner le réseau "Internet" 19, déplace le pointeur 6 du réseau "Internet " 19 vers la classe "classe" 30 et la sélectionne. Une ligne fléchée 41 colorée en vert est ainsi dessinée sur l'interface graphique 2, la pointe de la flèche étant orientée vers la classe "classe" 30. L'utilisateur procède de la même façon pour mettre en place une loi d'autorisation de la classe "classe" 30 vers le réseau "Internet" 19. Il dessine ainsi une autre ligne fléchée 42 colorée en vert, la pointe de la flèche étant orientée vers le réseau "Internet" 19. L'utilisateur a ainsi visualisé sur l'interface graphique que les équipements informatiques appartenant à la classe 30 "classe" du sous-ensemble du réseau 20a "Dmz", peuvent communiquer dans les deux sens avec les objets du réseau "Internet" 19.

Dans le deuxième cas, pour mettre en place une loi d'autorisation du réseau "Central" 20b vers la classe 30 "classe" et une loi d'interdiction de la classe 32 "classe-central-commerce" vers la classe 30 "classe", l'utilisateur procède comme précédemment, en spécifiant au moyen de la fenêtre de dialogue la loi d'autorisation et celle d'interdiction. Il dessine ainsi deux lignes fléchées, l'une 43 colorée en vert, l'autre 44 colorée en rouge. L'utilisateur a ainsi visualisé sur l'interface graphique que les équipements informatiques du réseau 20b "Central" peuvent communiquer avec le sous-ensemble des équipements informatiques du réseau 20a "Dmz", appartenant à la classe 30 "classe" mais que par contre les équipements informatiques des réseaux 20b "Central" et 20c "Commerce" appartenant à la classe 32 "classe-centra-commerce" ne peuvent pas communiquer avec le sous-ensemble des équipements informatiques du

réseau 20a "Dmz", appartenant à la classe 30 "classe". Lorsqu'il y a conflit de loi, c'est la loi d'interdiction qui l'emporte sur la loi d'autorisation.

L'utilisateur procède de manière itérative pour sélectionner les autres protocoles d'application et dessiner les lois de communication qui leur sont associés.

Le dessin de ces courbes fléchées représentatives des lois de communication permet de créer simultanément et instantanément la création des filtres associés aux routeurs filtrants et s'appliquant aux objets concernés. A cet effet, le terminal de calcul 1 comprend des moyens de calcul 1a pour convertir les données graphiques correspondant aux lois de communication en données de programmation des routeurs filtrants 8. Les données de programmation sont transférées du terminal de calcul 1, par la liaison 7, vers le routeur filtrant 8 dont les paramètres de filtrage sont ainsi automatiquement et rapidement réglés.

REVENDICATIONS

1. Procédé pour générer de manière simple et automatique les filtres, selon le protocole internet, destinés à éviter les risques d'intrusion des réseaux informatiques interconnectés ; ledit procédé comprenant la mise en oeuvre d'une interface graphique (2) pour, de manière itérative :

- créer (13, 14, 15) et visualiser (2) les objets (20, 25) et les classes (30, 32) du domaine de sécurité,

- sélectionner (12) et visualiser (18) les protocoles d'application (40) pour lesquels des filtres doivent être créés,

- dessiner (16) sur l'interface graphique (2), pour chaque protocole d'application (40) préalablement sélectionné, les lois de communication, au moyen de courbes fléchées (41, 42, 43, 44) reliant les objets et/ou les classes du domaine de sécurité,

(de sorte que le dessin de ces courbes fléchées permet de représenter les lois de communication du domaine de sécurité).

2. Procédé selon la revendication 1, tel que pour créer les filtres associés aux routeurs filtrants (25) et s'appliquant aux objets (20) concernés,

- on convertit les données graphiques représentatives des lois de communication en données de programmation des routeurs filtrants (8, 25).

3. Procédé selon l'une des revendications 1 ou 2, tel que pour modifier la politique de sécurité du domaine de sécurité,

- on modifie les lois de communication (41, 42, 43, 44) entre objets (20) ou classes (30) sur l'interface graphique (2), en sélectionnant des protocoles d'application prédéterminés.

4. Système pour générer de manière simple et automatique les filtres, selon le protocole internet, destinés à éviter les risques d'intrusion des réseaux informatiques interconnectés ; le dit système comprend une interface graphique (2) associée à un terminal de calcul (1) et des moyens de commande (4, 5) interagissant de manière itérative avec l'interface

graphique (2) pour :

- créer (13,14,15) et visualiser (2) les objets (20, 25) et les classes (30) du domaine de sécurité,

- sélectionner (12) et visualiser (18) les protocoles d'application (40) pour lesquels des filtres doivent être créés

- dessiner (16) sur l'interface graphique (2), pour chaque protocole d'application (40) préalablement sélectionné, les lois de communication ,au moyen de courbes fléchées (41, 42, 43, 44) reliant les objets et/ou les classes du domaine de sécurité,

(de sorte que le dessin de ces courbes fléchées permet de représenter les lois de communication du domaine de sécurité).

5. Système selon la revendication 4 tel que, pour créer les filtres associés aux routeurs filtrants (25) et s'appliquant aux objets concernés, le système comprend des moyens de calcul (1a) pour :

- convertir les données graphiques représentatives des lois de communication en données de programmation des routeurs filtrants (8, 25).

6. Système selon les revendications 4 ou 5 tel que, pour modifier la politique de sécurité du domaine de sécurité, les moyens de commande (4, 5) comportent des moyens pour sélectionner des protocoles d'application prédéterminés.

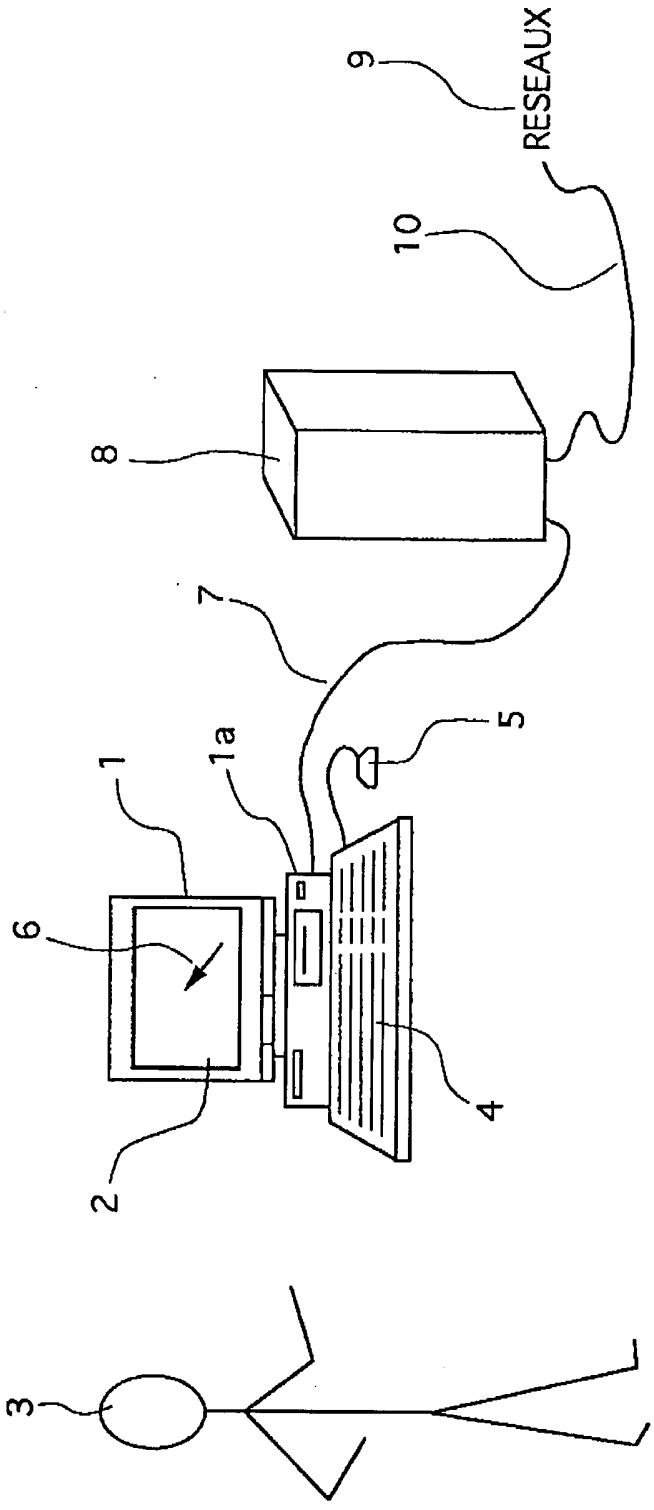


Fig. 1

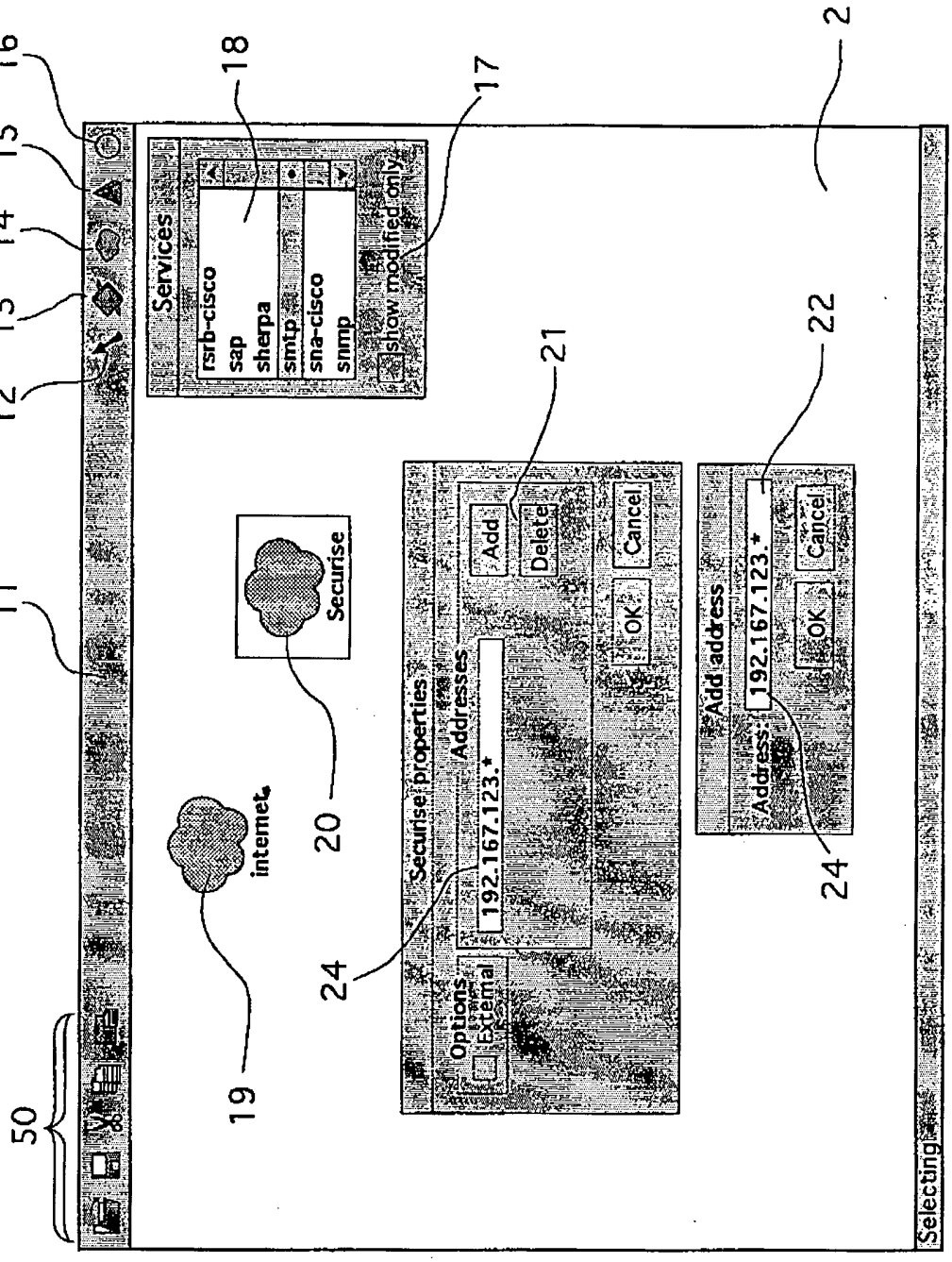

2
11
12
13
14
15
16
17
18
19
20
21
22
24
50
Services
rsrb-cisco
sap
sherpa
smtp
sna-cisco
snmp
show modified only
Securise
internet
Securise properties
Addresses
192.167.123.*
Add
Delete
OK
Cancel
Options
Add address
Address:
192.167.123.*
OK
Cancel
Selecting

Fig. 2

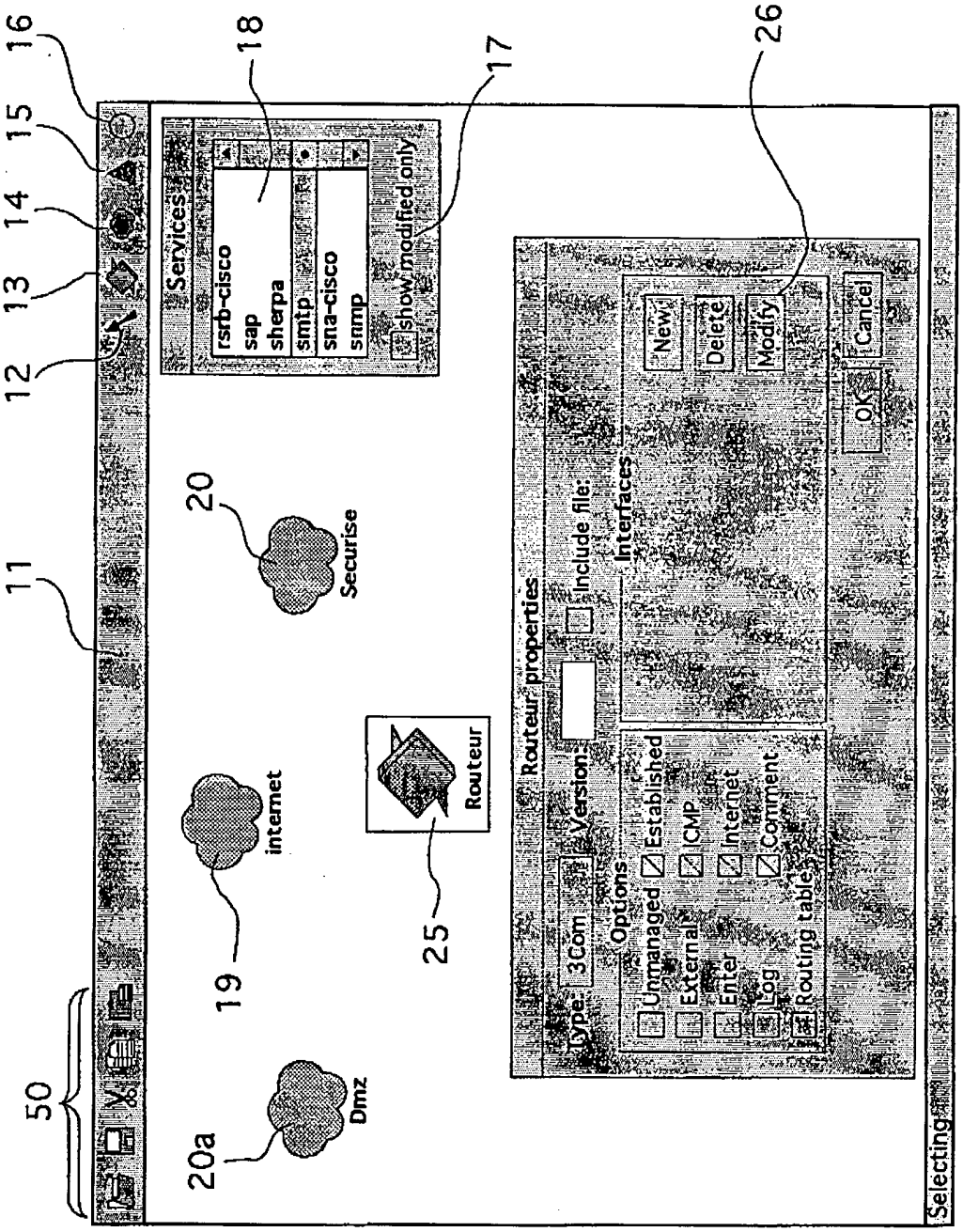

16
15
14
13
12
11
18
17
26
20
50
19
25
20a
Services
rsrb-cisco
sap
sherpa
smtp
sna-cisco
snmp
show modified only
Securise
internet
Routeur
Dmz
Routeur properties
Include file:
Interfaces
New
Delete
Modify
OK
Cancel
Type: 3Com
Version:
Options
Unmanaged
Established
External
ICMP
Enter
Internet
Log
Comment
Routing table
Selecting

Fig. 3

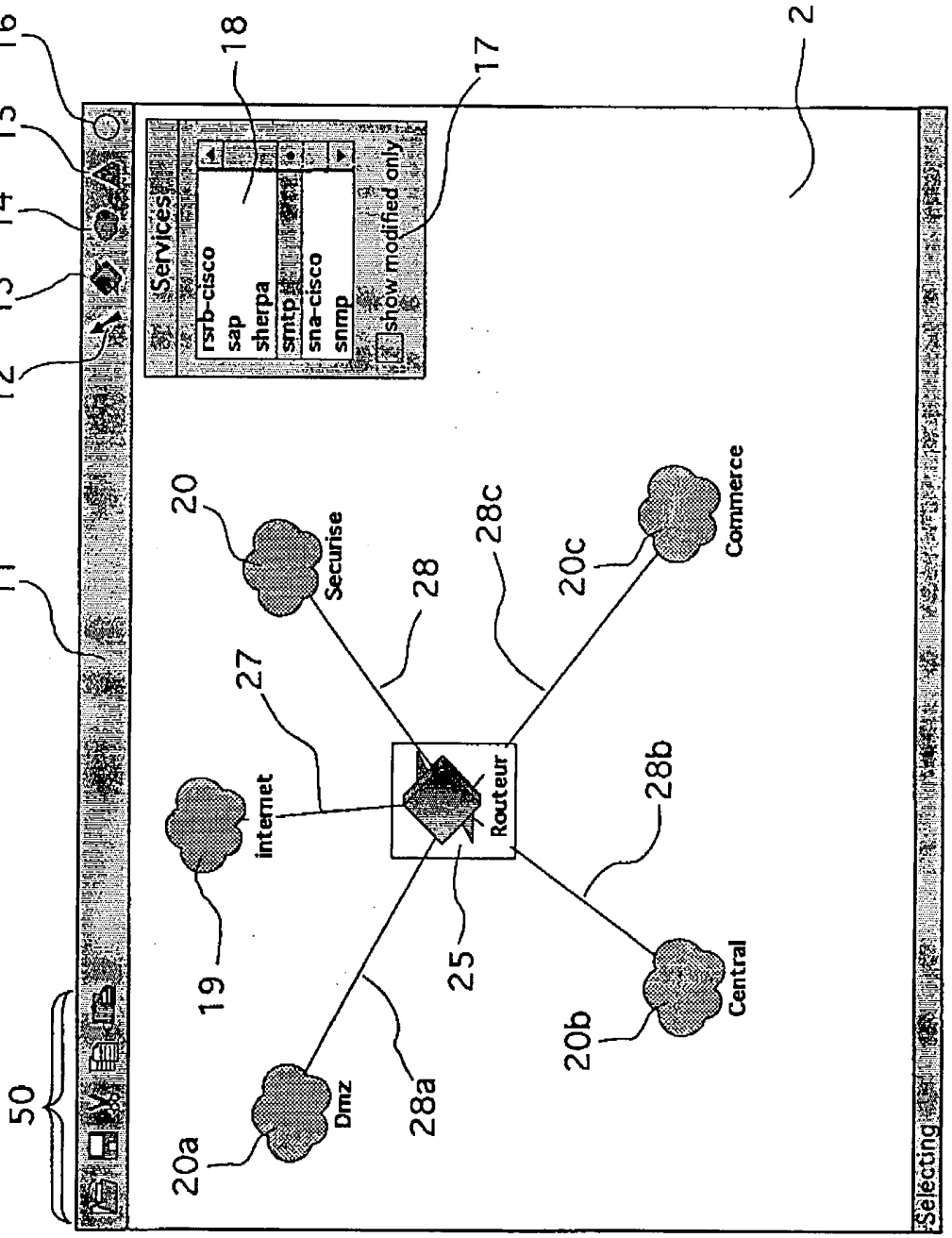

16
15
14
13
12
11
18
17
2
Services
rsrb-cisco
sap
sherpa
smtp
sna-cisco
snmp
show modified only
20
Securise
28
28c
20c
Commerce
27
internet
Routeur
28b
19
25
Central
20b
50
Dmz
28a
20a
Selecting

Fig. 4

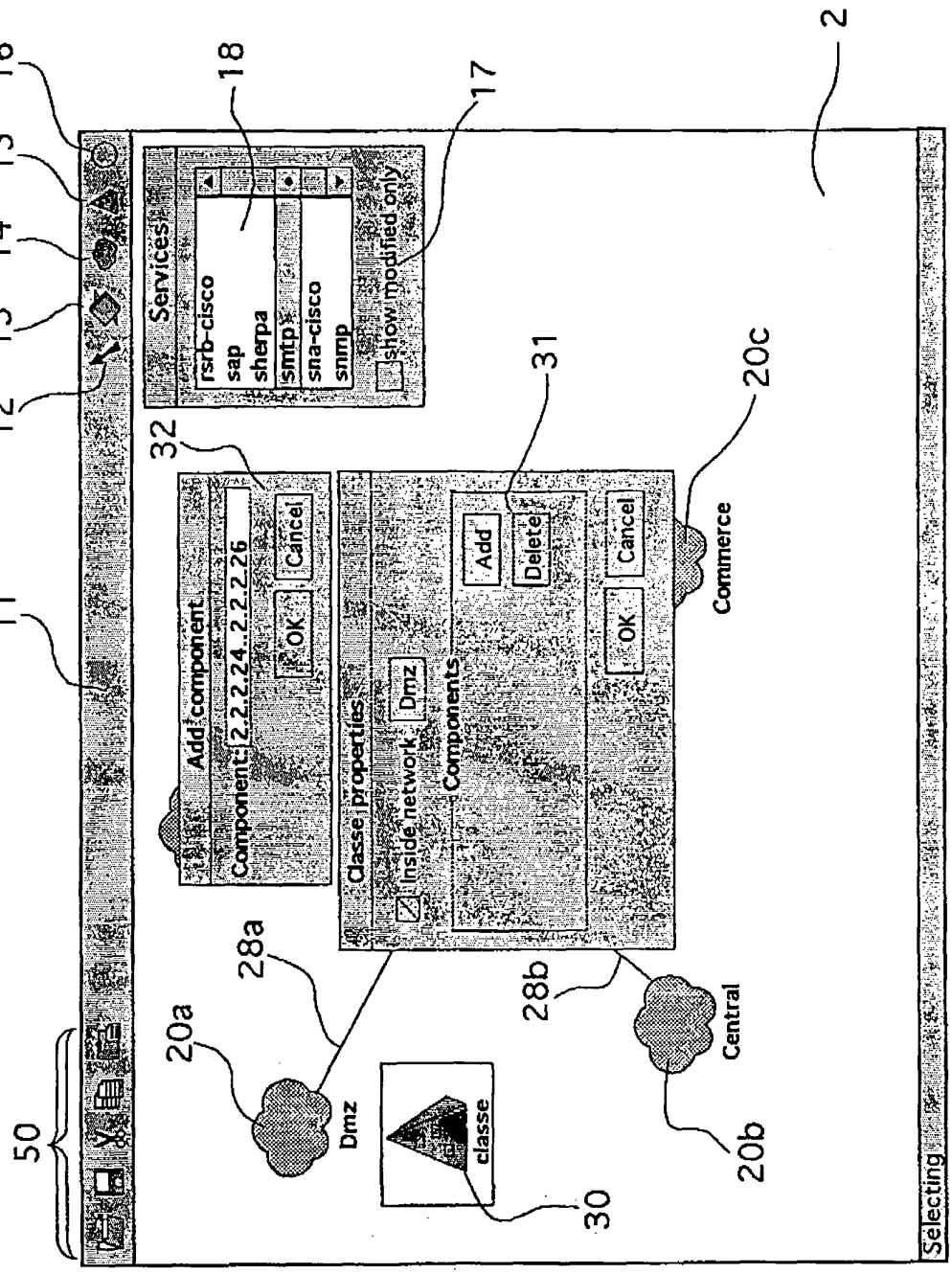

2
16
15
14
13
12
18
17
11
32
31
20c
28a
28b
20a
20b
50
30
Services
rsrb-cisco
sap
sherpa
smtp
sna-cisco
snmp
show modified only
Add component
Component: 2.2.2.24..2.2.2.26
OK
Cancel
Classe properties
Inside network
Dmz
Components
Add
Delete
OK
Cancel
Commerce
Dmz
classe
Central
Selecting

Fig. 5

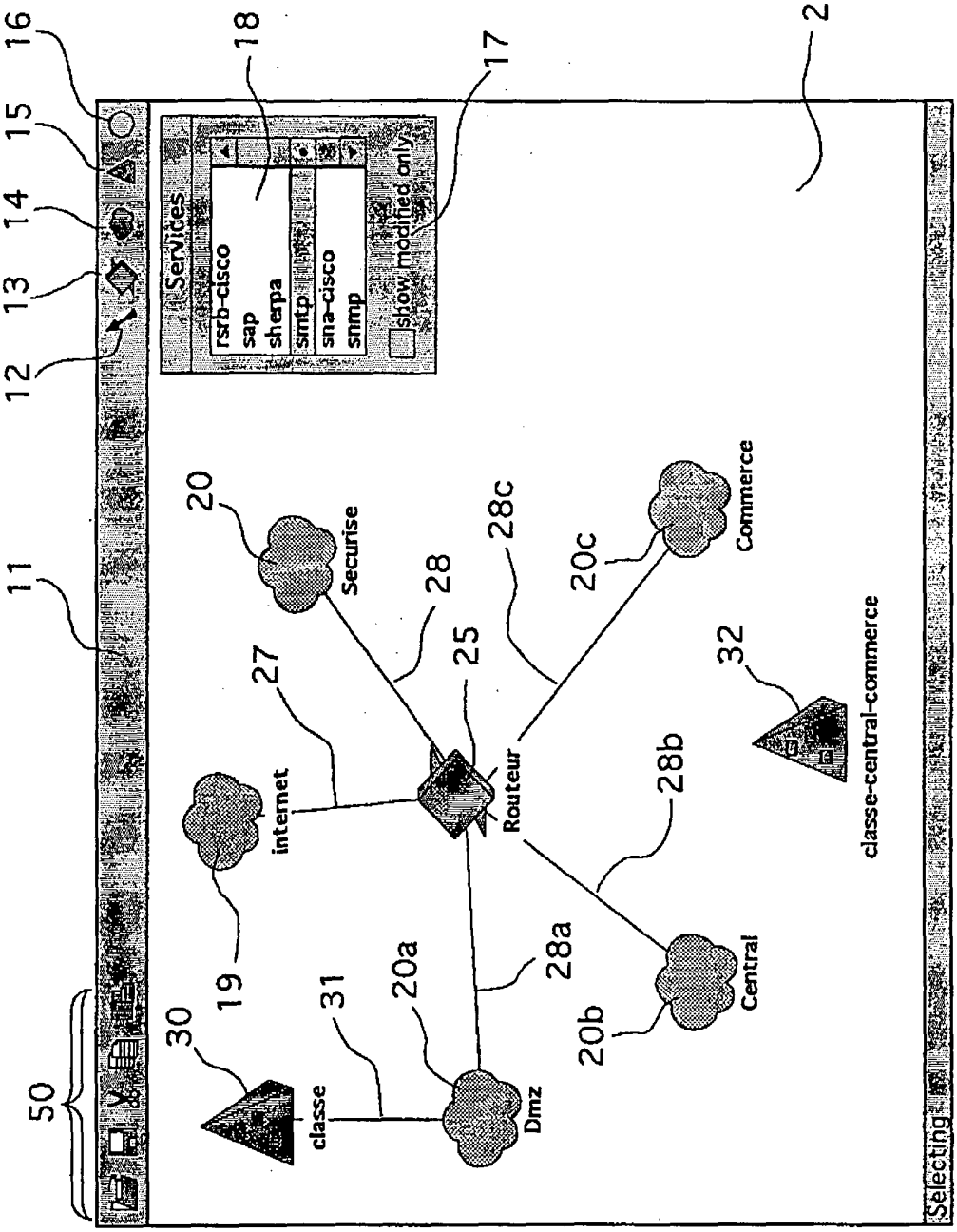

16
15
14
13
12
11
18
17
2
Services
rsrb-cisco
sap
sherpa
smtp
sna-cisco
snmp
show modified only
20
Securise
28
28c
20c
Commerce
27
25
32
internet
Routeur
28b
classe-central-commerce
19
30
31
20a
28a
20b
Central
classe
Dmz
50
Selecting

Fig. 6

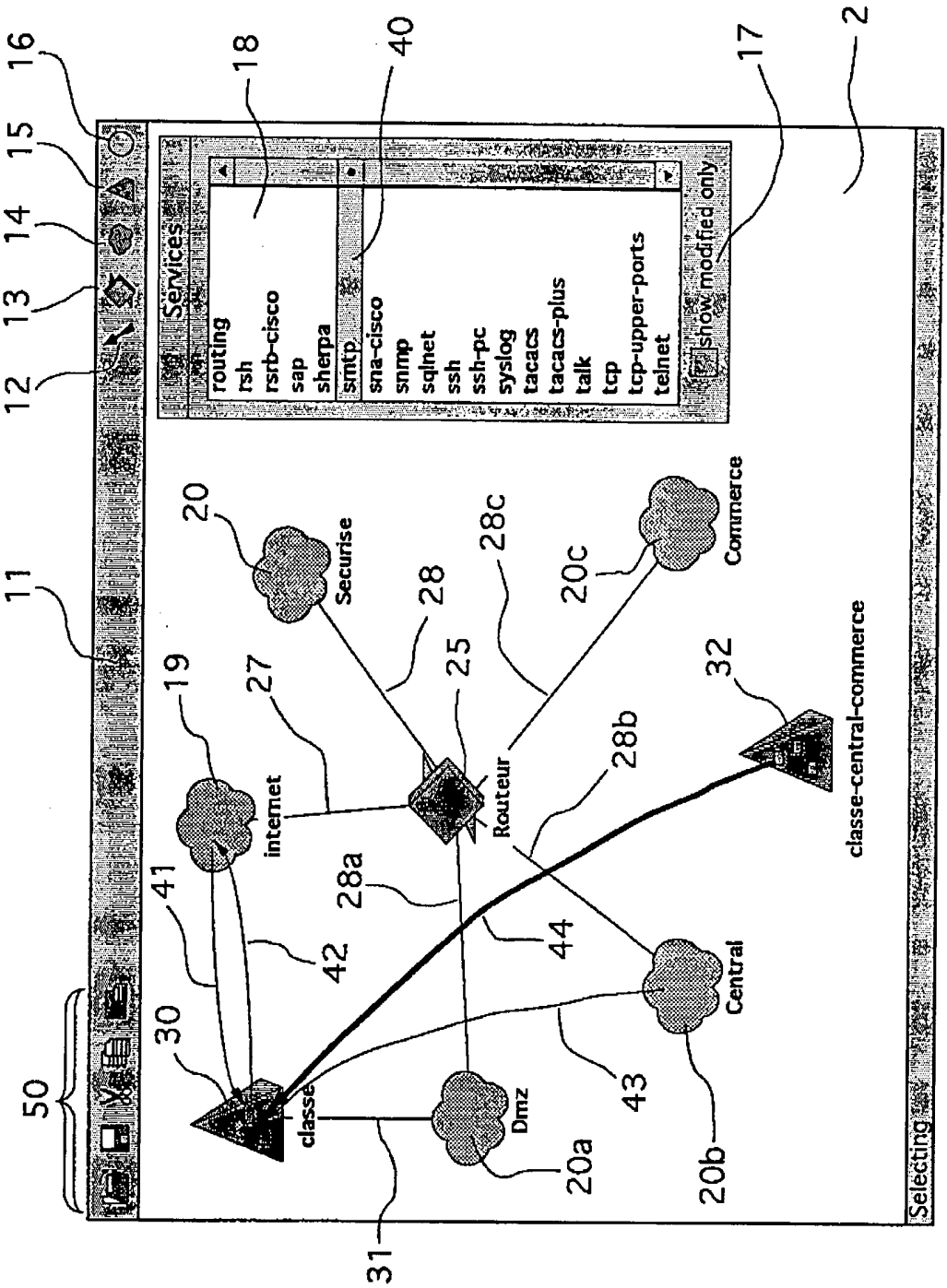

Services
routing
rsh
rsrb-cisco
sap
sherpa
smtp
sna-cisco
snmp
sqlnet
ssh
ssh-pc
syslog
tacacs
tacacs-plus
talk
tcp
tcp-upper-ports
telnet
show modified only
Securise
Commerce
internet
Routeur
classe-central-commerce
Central
Dmz
classe
Selecting
2
11
12
13
14
15
16
17
18
19
20
20a
20b
20c
25
27
28
28a
28b
28c
30
31
32
40
41
42
43
44
50

Fig. 7

INTERNATIONAL SEARCH REPORT

Interna l Application No
PCT/FR 98/02218

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06 H04L12/24 G06F9/44

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 658 837 A (CHECKPOINT SOFTWARE TECHN LTD) 21 June 1995 see abstract see page 3, line 36 - page 5, line 29; figures 2-4	1-6
A	HEYDON A ET AL: "MIRO: VISUAL SPECIFICATION OF SECURITY" IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, vol. 16, no. 10, 1 October 1990, pages 1185-1197, XP000162478 see page 1185, left-hand column, line 1 - right-hand column, paragraph 4 see page 1193, right-hand column, paragraph 4 - page 1195, paragraph 1; figures 13,14	1,4

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 December 1998	21/12/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Moens, R

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internat Application No
PCT/FR 98/02218

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	BACHMANN D W ET AL: "THE NETWORK MODELING TOOL: A DESIGN AID FOR LARGE-SCALE CAMPUS NETWORKS" PROCEEDINGS OF THE ANNUAL INTERNATIONAL PHOENIX CONFERENCE ON COMPUTERS AND COMMUNICATIONS, SCOTTSDALE, MAR. 21 - 23, 1990, no. CONF. 9, 21 March 1990, pages 560-567, XP000144586 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS see page 563, left-hand column, paragraph 2 - paragraph 4; figures 2A,2B	1,4
A	BELLOVIN S M ET AL: "NETWORK FIREWALLS" IEEE COMMUNICATIONS MAGAZINE, vol. 32, no. 9, 1 September 1994, pages 50-57, XP000476555 see page 51, left-hand column, line 18 - page 54, right-hand column, line 29	1-6

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interna l Application No
PCT/FR 98/02218

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0658837 A	21-06-1995	US 5606668 A	25-02-1997
		CA 2138058 A	16-06-1995
		WO 9700471 A	03-01-1997
		JP 8044642 A	16-02-1996
		US 5835726 A	10-11-1998

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 98/02218

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04L29/06 H04L12/24 G06F9/44

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 G06F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 0 658 837 A (CHECKPOINT SOFTWARE TECHN LTD) 21 juin 1995 voir abrégé voir page 3, ligne 36 - page 5, ligne 29; figures 2-4	1-6
A	HEYDON A ET AL: "MIRO: VISUAL SPECIFICATION OF SECURITY" IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, vol. 16, no. 10, 1 octobre 1990, pages 1185-1197, XP000162478 voir page 1185, colonne de gauche, ligne 1 - colonne de droite, alinéa 4 voir page 1193, colonne de droite, alinéa 4 - page 1195, alinéa 1; figures 13,14	1,4

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
15 décembre 1998	21/12/1998

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Moens, R

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 98/02218

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	BACHMANN D W ET AL: "THE NETWORK MODELING TOOL: A DESIGN AID FOR LARGE-SCALE CAMPUS NETWORKS" PROCEEDINGS OF THE ANNUAL INTERNATIONAL PHOENIX CONFERENCE ON COMPUTERS AND COMMUNICATIONS, SCOTTSDALE, MAR. 21 - 23, 1990, no. CONF. 9, 21 mars 1990, pages 560-567, XP000144586 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS voir page 563, colonne de gauche, alinéa 2 - alinéa 4; figures 2A,2B	1,4
A	BELLOVIN S M ET AL: "NETWORK FIREWALLS" IEEE COMMUNICATIONS MAGAZINE, vol. 32, no. 9, 1 septembre 1994, pages 50-57, XP000476555 voir page 51, colonne de gauche, ligne 18 - page 54, colonne de droite, ligne 29	1-6

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 98/02218

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0658837 A	21-06-1995	US 5606668 A	25-02-1997
		CA 2138058 A	16-06-1995
		WO 9700471 A	03-01-1997
		JP 8044642 A	16-02-1996
		US 5835726 A	10-11-1998